3. A method as defined in claim 1, said group being an additive group E(F_{2^M}) and said group operation being addition of points.

4. A method as defined in claim 1, said group being an additive group E(F_q), said group element being a point P with coordinates (x,y) on the elliptic curve, and said group operation being the scalar multiple kP of said point and an inverse element being the negative –P of said point.

5. A method as defined in claim 1, said integral value being a private key k.

6. A method of performing a selected group operation on a scalar and a selected element of said group, in a cryptographic processor, said method comprising the steps of :

representing said scalar as a binary vector;

recoding said binary vector to produce a signed digit representation of plus one and minus one digits;

selecting each of said recoded bits sequentially and for each of said selected bits performing said group operation on an intermediate element to derive a new intermediate element; and adding or subtracting said selected element to said intermediate element in accordance with said sign if said digit being selected; and

outputting said intermediate value as a result of said group operation.